bugkuCTF Writeup （Web）31-35

原创

Troublor 于 2018-01-31 15:29:26 发布 1541 收藏

分类专栏： CTF 文章标签： CTF Web PHP

本文链接：https://blog.csdn.net/troublor/article/details/79217918

各种绕过哟

代码审计

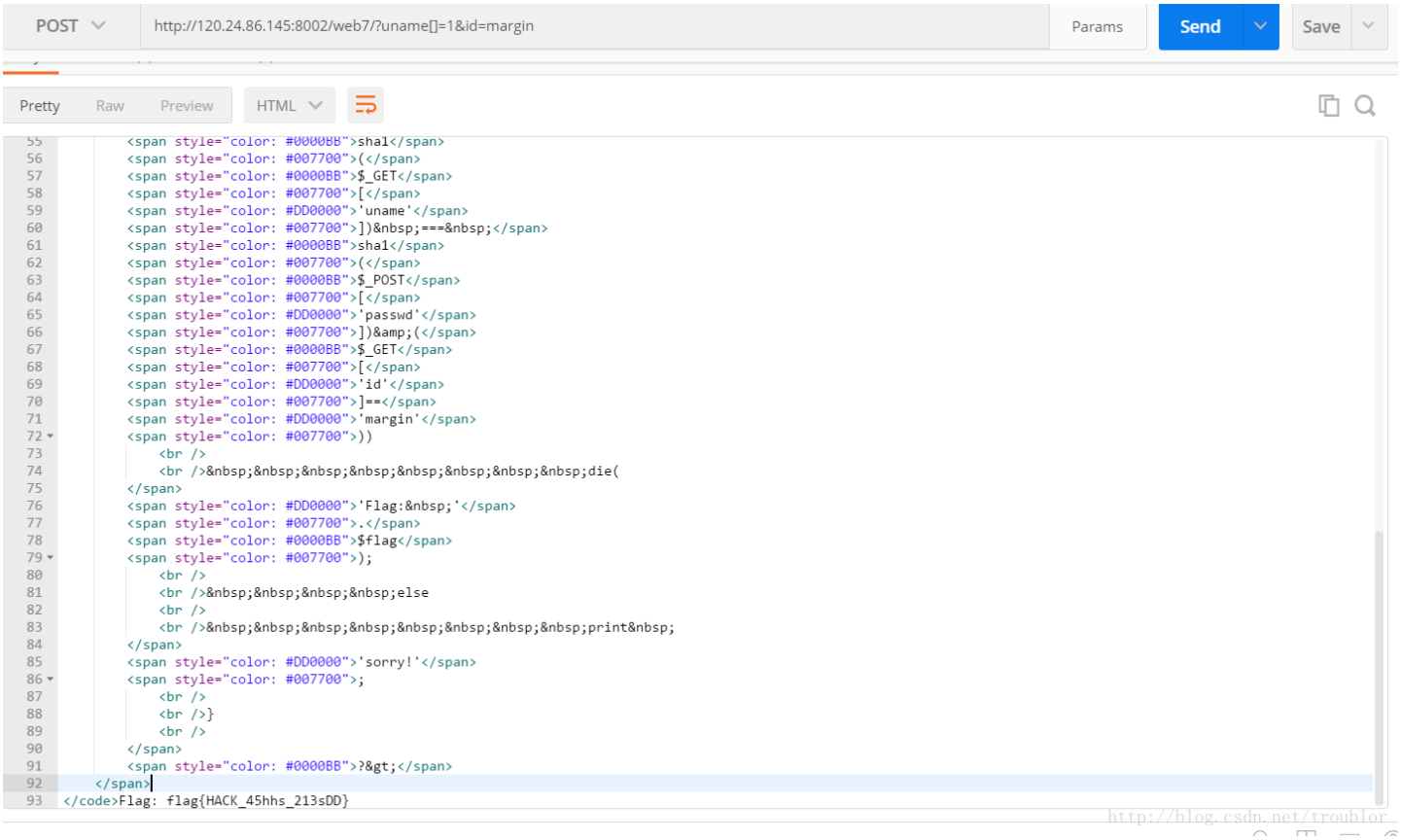
```php
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';

}
?>
```

用数组绕过sha1，传入uname和passwd都为数组

payload：`http://120.24.86.145:8002/web7/?uname[]=1&id=margin`

post：passwd[]=2

获得flag



Web8

代码审计

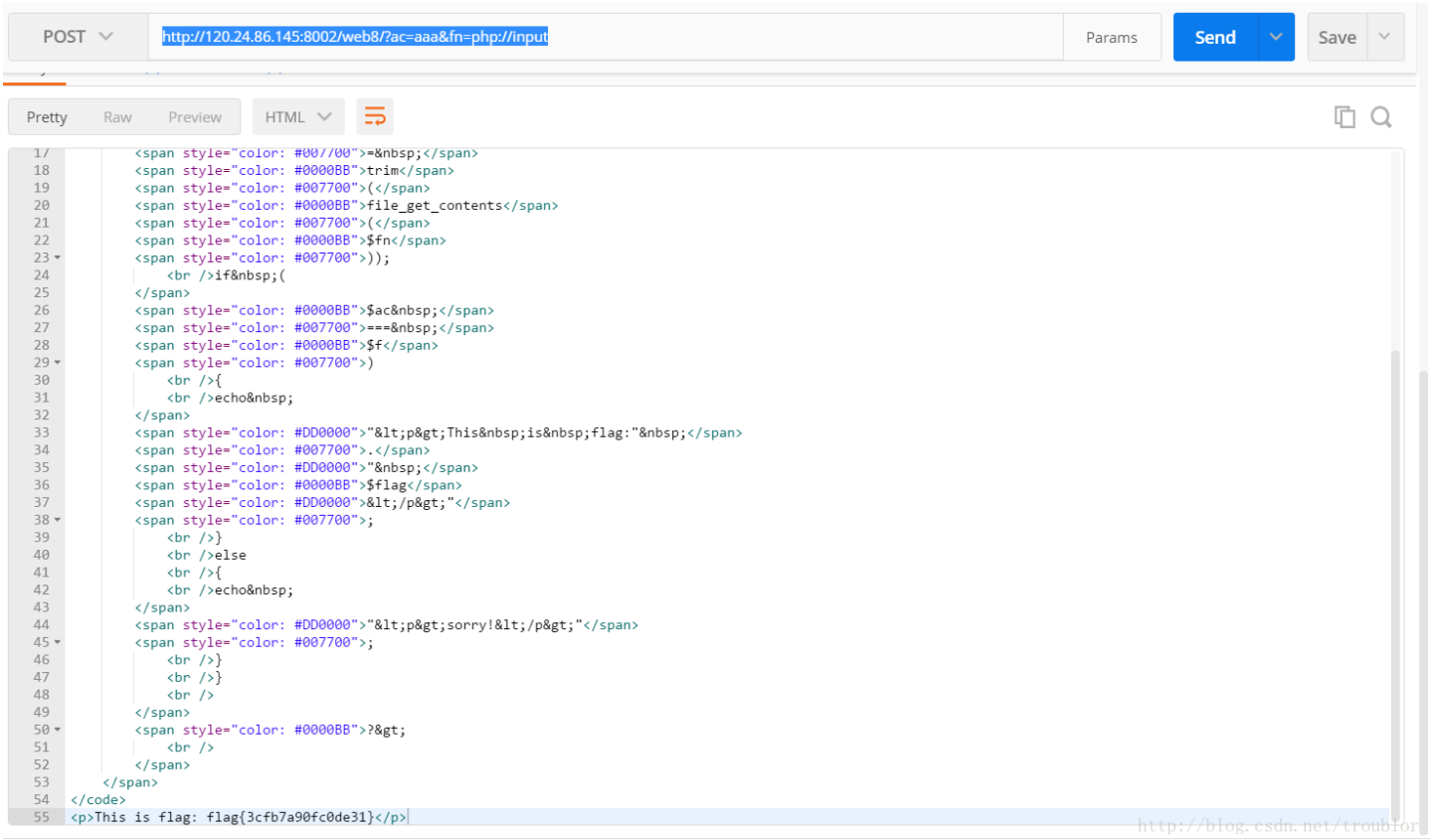
```php
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" ." $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

用php://input

payload：`http://120.24.86.145:8002/web8/?ac=aaa&fn=php://input`

postdata：aaa

得flag



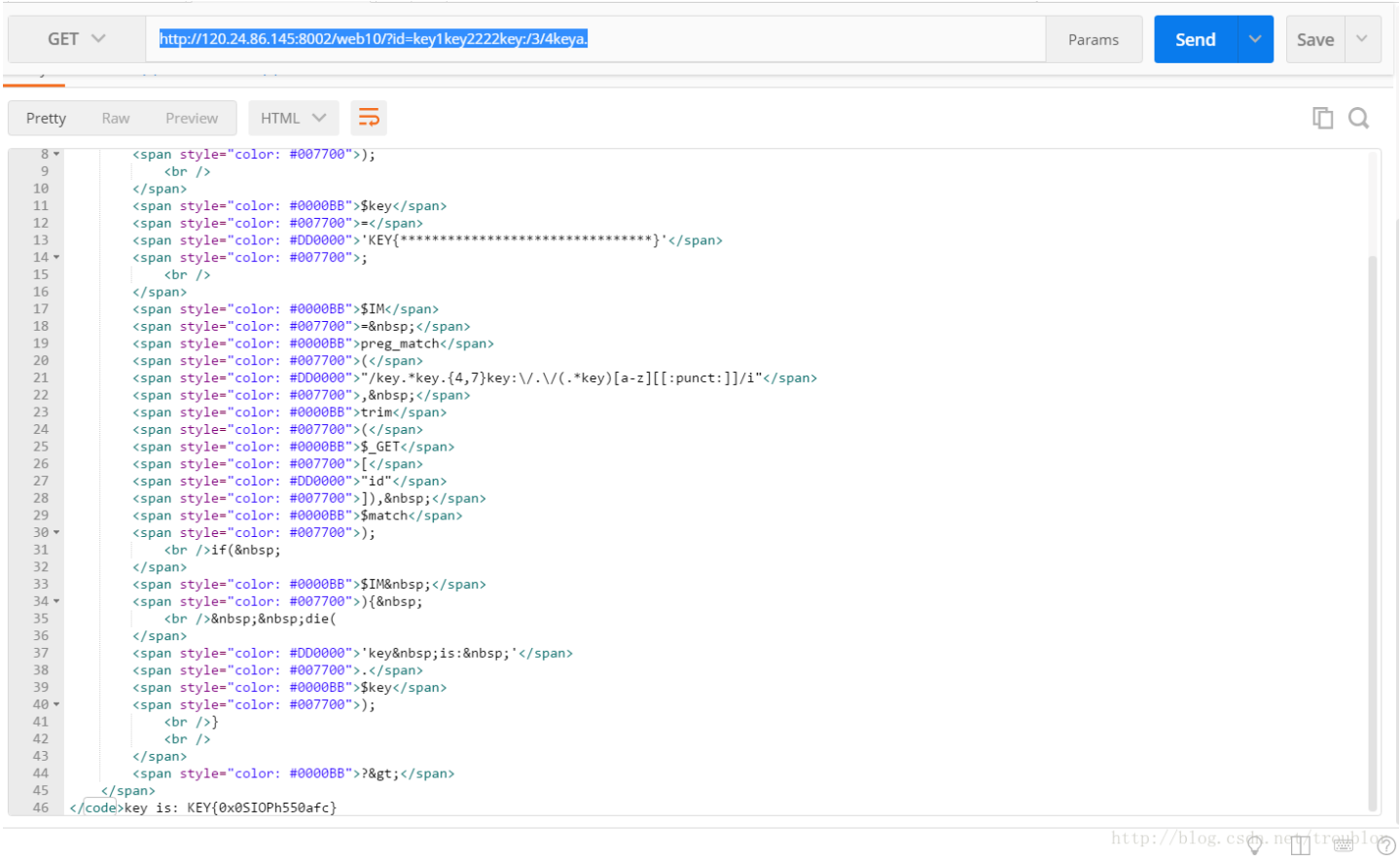
字符？正则？

代码审计

```php
<?php
highlight_file('2.php');
$key='KEY{********************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
  die('key is: '.$key);
}
?>
```

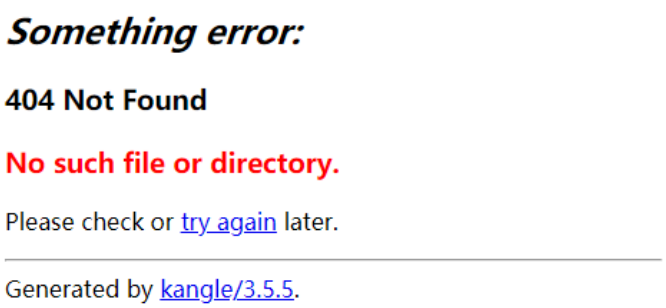
get的参数id只要满足正则表达式即可，很基础

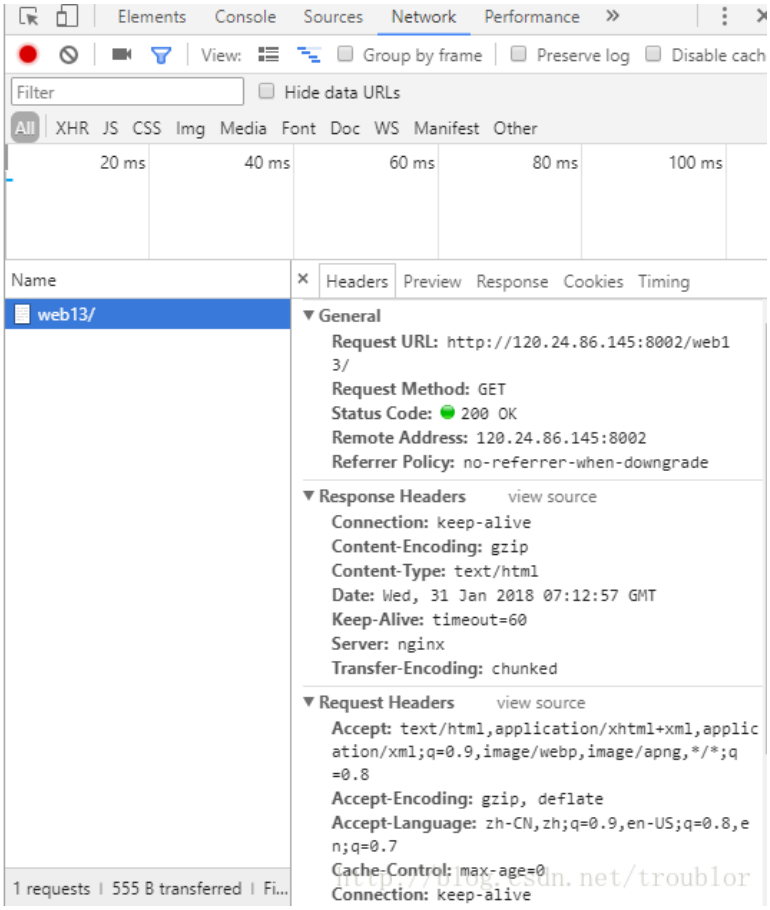
payload：`http://120.24.86.145:8002/web10/?id=key1key2222key:/3/4keya.`



考细心

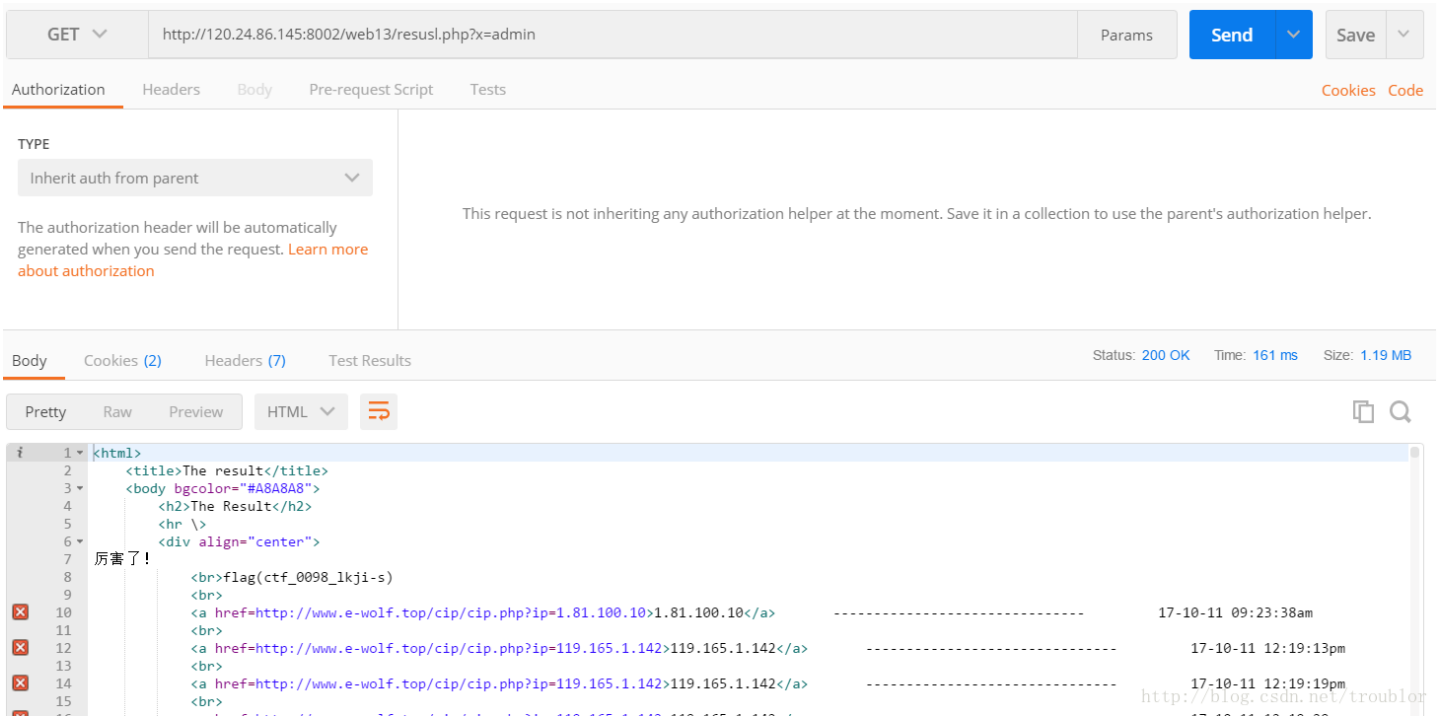
打开来看，是一个很假的404，看http相应果然是200





在这里很久也没找的有价值的线索
后来才知道网站根目录下有时候会放一个robots.txt来告诉各种爬虫哪些页面可以抓取，那些不行
这里就是查看这个txt，发现一个页面 `/resusl.php`
打开来看：

要提供get参数x
也没有什么头绪，只是题目提示里面说“想办法变成admin”，用admin作为x参数试了试，就成功了，想不到这题这么设置有什么意义



php代码审计

这题说还没弄好？也不知道是真是假，前面那么多题的各种脑洞让我的怀疑能力非常强大

点进去是代码审计

```php
 <?php

include "config.php";

class HITCON{
    private $method;
    private $args;
    private $conn;

    public function __construct($method, $args) {
        $this->method = $method;
        $this->args = $args;

        $this->__conn();
    }

    function show() {
        list($username) = func_get_args();
        $sql = sprintf("SELECT * FROM users WHERE username='%s'", $username);

        $obj = $this->__query($sql);
        if ( $obj != false  ) {
            $this->__die( sprintf("%s is %s", $obj->username, $obj->role) );
        } else {
            $this->__die("Nobody Nobody But You!");
        }

    }

    function login() {
        global $FLAG;

        list($username, $password) = func_get_args();
        $username = strtolower(trim(mysql_escape_string($username)));
        $password = strtolower(trim(mysql_escape_string($password)));

        $sql = sprintf("SELECT * FROM users WHERE username='%s' AND password='%s'", $username, $passwor
```

```php
        if ( $username == 'orange' || stripos($sql, 'orange') != false ) {
            $this->__die("Orange is so shy. He do not want to see you.");
        }

        $obj = $this->__query($sql);
        if ( $obj != false && $obj->role == 'admin'  ) {
            $this->__die("Hi, Orange! Here is your flag: " . $FLAG);
        } else {
            $this->__die("Admin only!");
        }
    }

    function source() {
        highlight_file(__FILE__);
    }

    function __conn() {
        global $db_host, $db_name, $db_user, $db_pass, $DEBUG;

        if (!$this->conn)
            $this->conn = mysql_connect($db_host, $db_user, $db_pass);
        mysql_select_db($db_name, $this->conn);

        if ($DEBUG) {
            $sql = "CREATE TABLE IF NOT EXISTS users (
                        username VARCHAR(64),
                        password VARCHAR(64),
                        role VARCHAR(64)
                    ) CHARACTER SET utf8";
            $this->__query($sql, $back=false);

            $sql = "INSERT INTO users VALUES ('orange', '$db_pass', 'admin'), ('phddaa', 'ddaa', 'user'
            $this->__query($sql, $back=false);
        }

        mysql_query("SET names utf8");
        mysql_query("SET sql_mode = 'strict_all_tables'");
    }

    function __query($sql, $back=true) {
        $result = @mysql_query($sql);
        if ($back) {
            return @mysql_fetch_object($result);
        }
    }

    function __die($msg) {
        $this->__close();

        header("Content-Type: application/json");
        die( json_encode( array("msg"=> $msg) ) );
    }

    function __close() {
        mysql_close($this->conn);
    }

    function __destruct() {
        $this->__conn();
```

```
            if (in_array($this->method, array("show", "login", "source"))) {
                @call_user_func_array(array($this, $this->method), $this->args);
            } else {
                $this->__die("What do you do?");
            }

            $this->__close();
        }

        function __wakeup() {
            foreach($this->args as $k => $v) {
                $this->args[$k] = strtolower(trim(mysql_escape_string($v)));
            }
        }
    }

    if(isset($_GET["data"])) {
        @unserialize($_GET["data"]);
    } else {
        new HITCON("source", array());
    }
```

这是要传入get参数data，然后利用unserialize的时候创建HITCON对象然后在程序运行结束的时候调用__destruct方法，进行注入，但是试了一下发现程序返回结果的逻辑好像和代码上显示的不太一样，可能真的是不能做吧。跳过了